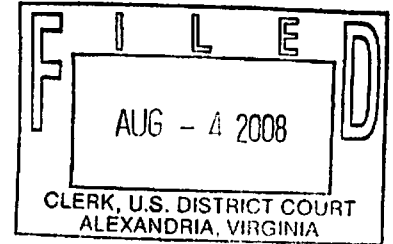


UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA



Alexandria Division

UNITED STATES OF AMERICA,

v.

CHIKEZIE ONWUMERE, HENRY OBILO,
BRANDY ANDERSON, OGECHUKWU
CHARLES ANYAKEE, and OBINNA ORJI

UNDER SEAL

Case No: 1:08mj604

UNDER SEAL

Affidavit in Support of a Criminal Complaint

I, Stephen E. Oakes, being first duly sworn, hereby depose and state:

1. I am a Special Agent with the FBI, and have been so employed for approximately three years and four months. Since that time I have received training in general law enforcement and in specialized areas including computer science, cyber investigations, and crime committed utilizing computers. I am currently assigned to a squad that investigates cyber intrusions within the Criminal Division of the FBI. I have participated in criminal investigations involving hacking, malicious code, domain name highjackings, botnets, and spamming. I have a computer science degree from Georgetown College and a law degree from the University of Kentucky, School of Law. Prior to my employment as a Special Agent, I was employed as a software developer for Affiliated Computer Systems in Lexington, Kentucky and as an assistant commonwealth's attorney for Fayette County, Kentucky. My current duties include the investigation of computer intrusions and other Federal criminal violations related to computers and the Internet.

2. I make this affidavit in support of a criminal complaint charging that CHIKEZIE ONWUMERE, HENRY OBILO, BRANDY ANDERSON, OGECHUKWU CHARLES

ANYAKEE, and OBINNA ORJI (collectively the Target Subjects) did, in the Eastern District of Virginia, commit offenses against the United States in violation of Title 18, United States Code, Section 1349 (Conspiracy to Commit Bank Fraud).

3. The information in this affidavit is based on (1) my personal knowledge and observations during the course of this investigation; (2) information conveyed to me by other law enforcement officials; (3) review of the evidence obtained from search warrants, pen registers and trap and trace devices, and subpoenas; (4) the review of call recordings; and (5) interviews with the Target Subjects. Since this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact known regarding this investigation.

DEFINITIONS OF COMPUTER-RELATED TERMS

4. The "Internet" is a collection of computers that are connected to one another via high-speed data links and telephone lines for the purpose of sharing information and services.

Connections between Internet computers may exist across state and international borders, even if those computers are in the same state.

5. Electronic mail (email) is a popular form of transmitting messages and/or files in an electronic environment between computer users. An Internet Protocol Address ("IP address") is a unique numeric address used to identify computers on the Internet. An IP address is comprised of a series of four numbers, each in the range of 0-255, separated by periods (e.g., 10.212.8.177). Every computer connection to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. An

IP address acts much like a home or business street address - it enables Internet sites to properly route traffic to each other.

6. An Internet Protocol Address ("IP address") is a unique numeric address used to identify computers on the Internet. An IP address is comprised of a series of four numbers, each in the range of 0-255, separated by periods (e.g., 10.212.8.177). Every computer connection to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. An IP address acts much like a home or business street address - it enables Internet sites to properly route traffic to each other.

7. Broadband Internet access refers to relatively high-speed connections allowing access to other computers on the Internet. Normally, the standard is a dial-up connection, while significantly faster connections are considered "broadband."

8. Wireless Internet access is accomplished without a physical cable attaching the computer to a network, e.g. the Internet, an Internet Service Provider, or a local network of some kind. Wireless cards allow a computer to connect to a local wireless hub in a home or business, or to a Wireless Cellphone Provider's network using cell towers. The wireless card and wireless receiver communicate by transmitting radio signals.

9. Caller-ID is a service provided by phone companies that displays the phone number of the caller on the receiver's phone or a special Caller-ID box. The display normally includes the caller's number and, if available, the directory listing for the caller, e.g. caller's name or business name.

THE SUBJECTS

10. TOBECHI ONWUHARA (ONWUHARA) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' accounts. ONWUHARA also organizes others who make such calls. ONWUHARA splits his time between Miami, Florida and Dallas, Texas. ONWUHARA is also known as Tobe or T. An arrest warrant from this Court is pending on ONWUHARA.

11. ABEL NNABUE (NNABUE) is primarily responsible for identifying potential victims and coordinating the gathering of information on victims. NNABUE resides in Dallas, Texas. NNABUE is also known as Que or Q. NNABUE was arrested on August 2, 2008 pursuant to an arrest warrant from this Court.

12. PAULA GIPSON (GIPSON) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' accounts and obtaining information on victims. GIPSON resides in Dallas, Texas. GIPSON was arrested on August 2, 2008 pursuant to an arrest warrant from this Court.

13. PRECIOUS NYA MATTHEWS (MATTHEWS) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' accounts and laundering the proceeds of the scheme. MATTHEWS is ONWUHARA's fiancée and lives in Miami, Florida. MATTHEWS was arrested on August 1, 2008 pursuant to an arrest warrant from this Court.

14. BEN KALU (KALU) is primarily responsible for providing information on victims. KALU lives in Baltimore, Maryland. An arrest warrant from this Court is pending on KALU.

15. OBINNA NNEJI (NNEJI) is primarily responsible for laundering money. NNEJI resides in Houston, Texas. An arrest warrant from this Court is pending on NNEJI.

16. EZENWA ONYEDEBELU (ONYEDEBELU) is primarily responsible for laundering money. ONYEDEBELU resides in Dallas, Texas. ONYEDEBELU was arrested on August 1, 2008 pursuant to an arrest warrant from this Court.

17. DONALD OKOROW (OKORO) is primarily responsible for laundering money. OKORO resides in Dallas, Texas. An arrest warrant from this Court is pending on OKORO.

18. MIKE WALTER (WALTER) is primarily responsible for organizing money mules in Asia and transferring the money back to the Target Subjects. WALTER resides in Jakarta, Indonesia and was arrested in Singapore as a result of this scheme on or about July 15, 2008.

19. CHIKEZIE ONWUMERE (ONWUMERE) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' accounts and laundering the proceeds of the scheme. ONWUMERE is also known as Cheeks or Chakiz. ONWUMERE resides in Brooklyn, New York.

20. HENRY OBILO (OBILO) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' accounts and laundering the proceeds of the scheme. OBILO resides in Miami, Florida.

21. BRANDY ANDERSON (ANDERSON) is primarily responsible for laundering the proceeds of the scheme. ANDERSON is the mother of one of NNABUE's children and they live together in Dallas, Texas.

22. OGECHUKWU CHARLES ANYAKEE (ANYAKEE) is primarily responsible for calling financial institutions and convincing them to wire transfer money out of victims' account

and laundering the proceeds of the scheme. ANYAKEE is also known as Charles Aneke.

ANYAKEE resides in Dallas, Texas.

23. OBINNA ORJI (ORJI) is primarily responsible for receiving funds from fraudulent wire transfers and laundering the proceeds of the scheme. ORJI was arrested in Arizona in relation to his activities in this scheme by local police in or about 2006. ORJI was released on bond and has since been a fugitive. ORJI resides in Dallas, Texas.

THE SCHEME

24. The Target Subjects are engaged in a scheme designed to defraud financial institutions. The Target Subjects normally target victims who have a large balance in a Home Equity Line of Credit (HELOC). The Target Subjects use the fraudulently-obtained personal information of the victims to initiate wire-transfers to over-seas bank accounts without the knowledge or authorization of the victims. Although each case is a little different, the following are the primary steps in the scheme.

25. The Target Subjects obtained pre-paid cell phones, Yahoo! email accounts, pre-paid wireless broadband PC cards, accounts with J2 Global Communications (J2), a fax-to-email service, accounts with E&M Enterprises (d/b/a/ Spoofcard.com) (Spoofcard), a Caller-ID spoofing service, and accounts with Listsource, a company that provides mortgage and real estate information.

26. NNABUE and others used Listsource to gather mortgage and real estate information, including information on potential victims who had large HELOC accounts. They would then make a copy of the victim's signature from the lease or loan documents. GIPSON, KALU, and

others would then run credit reports on the victims. The credit reports would show available balances on the HELOC accounts, as well as other personal information.

27. The Target Subjects would then use a pre-paid cell phone to call the victim's phone company and forward the victim's phone number to the pre-paid cell phone. The Target Subjects would use Spoofcard to make it appear that the call originated from the victim's phone.

28. ONWUHARA, GIPSON, MATTHEWS, ONWUMERE, OBILO, ANYAKEE, and others would call the victim's financial institution, normally a credit union, and use social engineering to obtain account information, including account numbers, balances, passwords, security questions, and the like. In some cases, the Target Subjects would use a laptop computer hooked up to a pre-paid wireless broadband card to access the victim's account over the Internet, using information obtained through the calls to the financial institution. ANDERSON was in the room at the time of many of these calls, although it is not known at this time if she participated in calling financial institutions.

29. ONWUHARA, GIPSON, MATTHEWS, ONWUMERE, OBILO, ANYAKEE, and others would then request a wire transfer from the victim's account to a bank account in Asia. As part of the financial institution's normal procedure, they would either fax or email an authorization form to the subjects. The Target Subjects would either have the form faxed to a number at J2 that would in turn email the form to the subjects, or they would have the bank email it to one of their Yahoo! accounts. The Target Subjects would fill out the form and cut and paste the electronic version of the victim's signature that they had previously acquired from Listsource. The Target Subjects would then fax the form back to the bank, normally through J2,

sometimes including a header at the top that made it appear that the fax came from the victim's phone.

30. Money transferred to banks in Asia was collected by money mules who got a cut of the incoming funds in return for opening business accounts, receiving money via wire transfers into those accounts, and then withdrawing the money and turning it over to couriers. The couriers bundled the money into containers and shipped the money to WALTER. WALTER would then send money transfers, normally via Western Union, to the Target Subjects, in amounts ranging from a thousand dollars up to tens of thousands of dollars. In addition, WALTER would send large transfers to ONWUHARA, including a transfer of €40,000,000.

31. MATTHEWS would transfer some of the money received to the other Target Subjects. In addition, ONWUHARA would go to casinos and deposit large sums of money, often in the hundreds of thousands of dollars. Days later, ONWUHARA would cash out approximately the same amount of money in the form of checks.

PROBABLE CAUSE

32. At 12:24 pm on December 7, 2007, an unidentified individual, impersonating Robert Short, called USSFCU, provided the correct personal information of Mr. Short and requested to make a wire transfer in the amount of \$280,000 dollars from Mr. Short's savings account to a Woori Bank of Korea account, ending in #1001, through the Wachovia Bank of New York.

33. As part of their normal business practice, USSFCU sent a wire transfer form to the caller. The caller asked that the form be sent to allstateassociates@yahoo.com. Upon receipt of the completed form, USSFCU sent the wire transfer to the Wachovia Bank of New York, and the

Wachovia Bank in turn wired the fund to the Woori Bank of Korea. The call was recorded as the regular business practice of the USSFCU, and was provided to the USSS and the FBI. Both Mr. Short and USSFCU are located in Alexandria, within the Eastern District of Virginia.

34. On December 9, 2007, the true Robert Short attempted to log onto the USSFCU Internet online banking but was not able to gain access due to a problem with the password. On December 10, 2007, Mr. Short contacted the USSFCU and was provided with a new password. Upon logging onto the Internet online banking, Mr. Short noticed that a total of \$280,000 dollars was missing and that several unauthorized Internet online transactions had been conducted in the checking account, the savings account and the Home Equity Line of Credit ("HELOC") account. Mr. Short notified the USSFCU of the discovery.

35. Pursuant to a subpoena, USSFCU provided the IP address that connected to Short's online account. The IP address came back to a pre-paid Verizon Wireless Broadband card with mobile telephone number (MTN) (954) 892-7434. In addition, Yahoo! Inc. ("Yahoo!"), in response to a subpoena, provided the same IP address as having accessed the email account: allstateassociates@yahoo.com.

36. Pursuant to a subpoena, Verizon provided video footage showing three men depositing \$200 in cash at a Verizon store in Plano, Texas for the Verizon broadband account with MTN (954) 892-7434. A cooperating witness, who was a former associate with ONWUHARA and NNABUE, identified ONWUHARA and NNABUE as two of the three individuals in the video footage from Verizon. The third individual was later identified as ONYEDEBELU by his DMV photograph.

37. Further investigation revealed that the Target Subjects were using the services of Spoofcard, a company that provides Caller-ID spoofing, call recording, and voice masking

services. The Target Subjects would call Spoofcard's toll-free number and enter a PIN. They would then specify the recipient's phone number and the number they wished to display on the recipient's Caller-ID box.

38. The investigation has also uncovered additional victim banks and credit unions in which the same methods, Spoofcard PINs, e-mail addresses, and pre-paid cell phones have been used to conduct the fraud. Pursuant to a search warrant issued by this Court, the FBI and USSS have obtained and listened to recordings of calls made by the Target Subjects. The agents were able to differentiate the voices of several men and two women. In all, dozens of financial institutions have been identified as victims of this scheme as a result of the calls through Spoofcard, and losses approach \$7.9 million and total attempted losses exceed \$24,500,000.

39. A review of telephone recordings provided by Spoofcard identified a call placed on November 10, 2007 at approximately 17:49 EST, from the same individual who called USSFCU on December 7, 2007. The caller used the Spoofcard service to disguise his telephone number, 214-240-9841, as that of a local physician. The subject contacted CVS Pharmacy, 3900 Forest Lane, Dallas, Texas, impersonated Dr. Mc Elya, and made a request for a prescription of Valtrex (500mg) for TOBE ONWUHARA.

40. On November 17, 2007 at approximately 18:50:40 EST, the same individual again used the Spoofcard service to disguise telephone number 214-240-9841. This time the subject contacted CVS Pharmacy, 4610 Frankfort Road Dallas, Texas and impersonated Dr. McElya to request a prescription of Valtrex (500 mg). The prescription was to be picked up by TOBE ONWUHARA, using ONWUHARA's birth date.

41. On April 10, 2008, pursuant to a sneak-and-peek search warrant issued by United States Magistrate Judge Joan M. Azrack, Eastern District of New York, ONWUHARA, NNABUE,

MATTHEWS, and OBILO were stopped together and interviewed at JFK International Airport on their return to the United States from Nigeria. During a conversation with ONWUHARA, agents recognized ONWUHARA's voice as the same voice on calls to USSFCU on December 7, 2007 that resulted in the fraudulent and unauthorized transfer of \$280,000 from the account of Robert Short. ONWUHARA was in possession of the cellular telephone with phone number 214-240-9841 at the time of the interview.

42. On the same date, during a conversation with MATTHEWS, MATTHEWS confirmed that ONWUHARA went by the nickname T or Tobe, and that NNABUE went by the nickname Q or Que. Agents recognized MATTHEWS's voice as one of the female callers on calls to financial institutions requesting wire transfers.

43. Pursuant to a search warrant, Yahoo! provided the contents of email account tobeohara@yahoo.com, which had received email from allstateassociates@yahoo.com in reference to the current scheme. The contents of the account included messages to an individual in Indonesia named "Mike." The individual in Indonesia stated that he could get access to accounts in Korea, China, Hong Kong, Singapore, and Indonesia and would split the proceeds 40% / 60%

44. Suspicious Activity Reports (SARS) show money being sent via wire transfer from WALTER in Indonesia to MATTHEWS and others. After her arrest on August 1, 2008, MATTHEWS confirmed that the money coming in from overseas constituted the proceeds from this scheme. MATTHEWS wire transferred cash received from overseas to the other Target Subjects.

45. Pursuant to a subpoena, Bank of America produced bank statements for MATTHEWS's accounts. A review of those accounts showed the following transactions.

- a. On or about January 22, 2008, MATTHEWS received a wire transfer for \$110,000 from Indonesia into her bank account.
- b. On or about January 22, 2008, MATTHEWS wire transferred \$25,000 to ANDERSON.
- c. On or about May 20, 2008, MATTHEWS received \$99,961.50 via wire transfer from Nigeria into her bank account.
- d. On or about May 21, 2008, MATTHEWS wire transferred money to ONWUMERE, ONYEDEBELU, NNABUE, ANYAKEE and OKORO, totaling \$21,124.


46. As noted above, four members of the conspiracy were arrested between August 1 and 2, 2008, pursuant to arrest warrants issued by this Court. Conversations with those conspirators confirmed that ORJI was used as a money mule and was arrested in Phoenix, Arizona in connection with activities relating to the current scheme. In addition, ONYEDEBELU bailed out ORJI who has been a fugitive ever since. ORJI would open bank accounts into which funds from victims were transferred and then ORJI would withdraw the money and send a portion to ONWUHARA.

47. Conversations with the conspirators after their arrest also revealed that ANDERSON was present during numerous sessions at which the conspirators made calls to financial institutions as part of this scheme. Although there is no evidence at this time that ANDERSON placed any calls, she was aware of the nature of the sessions. In addition, it was confirmed that OBILO, ANYAKEE and ONWUMERE made multiple calls to financial institutions in order to facilitate the fraudulent transfer of funds overseas.

CONCLUSION

48. Based upon the forgoing, I have probable cause to believe from in or about September 2007, and continuing through in or about July 2008, in the Eastern District of Virginia and elsewhere, CHIKEZIE ONWUMERE, HENRY OBILO, BRANDY ANDERSON, OGECHUKWU CHARLES ANYAKEE, and OBINNA ORJI did knowingly conspire to execute a scheme or artifice to defraud a financial institution and to obtain any of the moneys, funds, credits, assets, securities, and other property owned by, and under the control and custody of, a financial institution, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1349.

I therefore request a warrant be issued to any duly authorized Officer of the United States to arrest CHIKEZIE ONWUMERE, HENRY OBILO, BRANDY ANDERSON, OGECHUKWU CHARLES ANYAKEE, and OBINNA ORJI.


Stephen E. Oakes
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this 4th day of August, 2008 at Alexandria, VA.

 /s/
John F. Anderson
United States Magistrate Judge